AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings of claims in the application:

1. (Currently Amended): A method for validating a client device by a server device, said method comprising the steps of:

generating a shared unpredictable secret;

storing the shared unpredictable secret in the client device and in the server device;

requiring the client device to prove that it holds a correct secret as a precondition to the server device validating the client device; and

replacing the shared unpredictable secret by a new shared unpredictable secret when the server device validates the client device [[.]] , wherein:

the server device sends update data to the client device;

the client device applies the update data to the shared unpredictable secret to generate a new secret; and

the client device replaces the shared unpredictable secret with the new secret.

2. (Original): The method of claim 1 wherein an initial shared unpredictable secret is determined in the client device and in the server device during a registration step that occurs prior to a log-in step.

3. (Currently Amended): The method of claim 2 wherein the registration step entails more checking of ~~bona fides of~~ authentication data presented by the client device than does [[a]] the log-in step.

4. (Original): The method of claim 2 wherein, during the registration step, the client device is required to make a payment to the user device.

5. (Currently Amended): The method of claim 1 wherein the shared unpredictable secret is generated by a generator from ~~the~~ a group comprising a random number generator and a pseudo-random number generator.

6. (Original): The method of claim 1 wherein the shared unpredictable secret comprises an unpredictable component and a fixed component.

7. (Original): The method of claim 1 wherein a plurality of client devices desire to be validated by the server device; and each client device has a unique unpredictable secret that it shares with the server device.

8. (Currently Amended): The method of claim 1 wherein, following a validation of the client device, the server device discards the ~~original~~ shared unpredictable secret and stores within the server device [[a]] the new shared unpredictable secret that can be generated by applying the update data to the ~~original~~ shared unpredictable secret.

9. (Cancelled).

10. (Currently Amended): The method of claim [[9]] 1 wherein:

the server device generates the update data using a generator from ~~the~~ a group comprising a random number generator and a pseudo-random number generator; and the step of applying the update data to the shared unpredictable secret comprises computing a one-way function of ~~the~~ a combination of the shared unpredictable secret and the update data.

11. (Currently Amended): The method of claim [[9]] 1 wherein the client device sends acknowledgement data to the server device to confirm that the client device has replaced the shared unpredictable secret with the new secret.

12. (Currently Amended): The method of claim 11 wherein, in response to the server device receiving the acknowledgement data from the client device, the server device:

validates the client device; and

discards the shared unpredictable secret and stores within the server device the new secret, which now becomes [[a]] the new shared unpredictable secret.

13. (Currently Amended): The method of claim 11 wherein:

the client device sends to the server device proof data demonstrating that the client device holds [[a]] the correct secret; and

the server device is adapted to accept from the client device any proof data that are generated from a secret that is newer than the secret for which the most recent acknowledgment data have been received by the server device.

14. (Original): The method of claim 11 wherein:

the client device sends to the server device both the acknowledgment data and proof data derived from the new secret.

15. (Original): The method of claim 14 wherein:

the proof data are computed on the new secret; and

the proof data serve also as the acknowledgment data.

16. (Currently Amended): The method of claim 1 wherein:

the client device presents proof data to the server device, wherein the proof data are derived from [[a]] the shared unpredictable secret using a proof data generation algorithm, and the proof data do not divulge the shared unpredictable secret;

the server device checks the proof data by using a proof data generation algorithm consistent with the proof data generation algorithm used by the client device; and

when the server device determines that the proof data presented by the client device were not generated from the ~~same~~ shared unpredictable secret that is stored in both the client device and in the server device, the server device does not validate the client device.

17. (Original): The method of claim 16 wherein each proof data generation algorithm is a one-way function.

18. (Currently Amended): A system for enabling a server device to validate a client device, said system comprising:

at least one client device;

a server device;

a shared unpredictable secret;

means for storing the shared unpredictable secret in the client device;

means for storing the shared unpredictable secret in the server device;

coupled to the client device and to the server device, means for determining whether the client device holds a correct secret;

coupled to the determining means, means for allowing the server device to validate the client device when the client device proves that it holds a correct secret; and

coupled to the client device and to the server device, means for replacing the original shared unpredictable secret with a new shared unpredictable secret when the server device validates the client device [[.]] , said means for replacing further comprising:

means for the server device to send update data to the client device;

means for the client device to apply the update data to the shared unpredictable secret to generate a new secret; and

means for the client device to replace the shared unpredictable secret with the new secret.

19. (Currently Amended): A computer readable medium containing computer program instructions for enabling a server device to validate a client device, said computer program instructions causing the execution of the following steps:

generating a shared unpredictable secret;

storing the shared unpredictable secret in the client device and in the server device;

requiring the client device to prove that it holds a correct secret as a precondition to allowing the client device to be validated by the server device; and

replacing the shared unpredictable secret by a new shared unpredictable secret when the client device is validated by the server device[[.]] , wherein:

the server device sends update data to the client device;

the client device applies the update data to the shared unpredictable secret to generate a new secret; and

the client device replaces the shared unpredictable secret with the new secret.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]